July 1995/Number1-95

security awareness bulletin

Inside

National Industrial Security Program

Department of Defense Security Institute, Richmond, Virginia

security awareness bulletin

Approved for open publication Unlimited reproduction authorized

Director
Department of Defense Security Institute
R. Everett Gravelle

Editor
Lynn Fischer

The Security Awareness Bulletin is provided by the Department of Defense Security Institute, Richmond, Virginia. Primary distribution is to DoD components and contractors cleared for classified access under the Defense Industrial Security Program and special access programs. Our purpose is to promote security awareness and compliance with security procedures through dissemination of information to security trainers regarding current security and counterintelligence developments, training aids, and education methods.

New distribution, address changes:

Government agencies: DoD Security Institute, Attn: SEAT, 8000 Jefferson Davis Hwy, Richmond, VA 23297-5091, POC Tracy Gulledge, (804) 279-4223, DSN 695-4223; fax (804) 279-6406, DSN 695-6406.

DIS activities: HQ DIS/V0951, 1340 Braddock Place, Alexandria, VA 22314-1651.

DISP contractors: Automatic distribution to each cleared facility. Send change of address to your DIS field office.

Introducing the National Industrial Security Program

This issue of the *Bulletin* is devoted entirely to the inauguration of the National Industrial Security Program (NISP) which fulfills the vision of many in both government and industry who several years ago proposed that the Executive Branch of government have a common standard for industrial security. The NISP was conceived to eliminate conflicting, redundant, and unnecessary requirements through standardization of policies and procedures, coupled with interagency reciprocity.

The guiding document for this government-wide program, the National Industrial Security Program Operating Manual (NISPOM) was signed in late 1994 by the Deputy Secretary of Defense and promulgated in early 1995. Administration of the Program within DoD by the Defense Investigative Service is to support the national security strategy of the United States by working in partnership with industry to develop and maintain security systems which provide critical technology with a level of protection that is rational, threat-appropriate, and cost-effective.

Since the NISPOM replaces the Department of Defense Industrial Security Manual, it is important for all of us to focus on the important changes in this program. With the assistance of the Office of the Secretary of Defense, Industrial Security staff, the DoD Security Institute's Industrial Security Team has summarized some of the more significant changes.

DoDSI's Industrial Security Team has also revised and improved the Self-Inspection Handbook, first issued in February 1992 as an issue of the *Bulletin*. The Handbook, developed to assist FSOs in the internal evaluation and review of their facility's security posture, promises to be an invaluable tool for security professionals in industry as they come to terms with the risk management philosophy underlying the new and leaner NISPOM.

The DoD Self-Inspection Handbook
TABLE OF CONTENTS

DoD CONTRACTOR SELF-INSPECTION HANDBOOK

The Contractor Security Review Requirement

Contractors shall review their security system on a continuing basis and shall conduct a formal self-inspection at intervals consistent with risk management principles. **[1-207, NISPOM]**

The Contractor Self-Inspection Handbook

The National Industrial Security Program Operating Manual (NISPOM) requires all participants in the NISP to conduct their own security reviews (self-inspections). This handbook is an updated version of the Self-Inspection Handbook first published in February of 1992. It contains the NISPOM's requirements in check list form, explains their arrangement into the "Elements of Inspection," and suggests various techniques to enhance the quality of your reviews.

The Self-Inspection check list is a list of the more prominent NISPOM security requirements in question form. The answer to each can be located within the NISPOM paragraph citation given at the end of each question. Your immediate task is to determine which of these requirements relates to your security program. These questions are located within alphabetically delineated areas (A thru V), of common security concern. Traditionally known as the *"Elements of Inspection,"* they combine to make up your Self-Inspection check list.

The first three Elements of Inspection: (A) Facility Clearance, (B) Access Authorizations, and (C) Security Education must be covered during the inspection of all cleared facilities. Any remaining elements need only be covered if they relate to your security program. The easiest and quickest way to determine this is to ask the I.S. Representative which elements were covered during the last inspection. A look at your SPP (if you have one) will also provide clues. Of course, as your program becomes more involved with classified (e.g., changing from a non-possessing to a possessing facility), you'll have to expand your review process to include those new elements of inspection. Remember also that not all of the questions (requirements) within each relevant area relate to your program. The best way to determine this is to review each question (requirement) in the context of your industrial security program. If your involvement with classified invokes the requirement, your procedures should comply with it. Reading each question in the relevant areas of inspection is a good way to become knowledgeable of the Manual's requirements.

Inspection Techniques

To get a clear picture of the state of security at your facility you must (1) know the requirements by which you are inspected (this is where the check list will help), (2) know your facility's physical layout (i.e., where the classified is stored, worked on, etc.), and (3) have knowledge of the processes involved in the classified programs at your facility. Remember, your primary sources of information are ***documents*** and ***people***.

Your job as an inspector is to *verify* and *validate* that your facility security program is properly protecting classified. To do this you simply review the self-inspection questions against appropriate documentation, people and their actions, and classified information involved in the facility's industrial security program. This is where the self-inspection check list comes in handy. It not only gives you the Manual's

requirements, but it organizes them into elements of common security concern. These elements should not be held mutually exclusive during the inspection process. In fact, it will become obvious to you that they frequently interrelate.

Questioning Techniques

A quality self-inspection depends on your ability to ask questions which may identify security problems. Seek information about *current* procedures, but also about *change* which could affect future actions. Get out of your office and into the facility working environment. Talk to the people!

- ❑ All questions should be considered in the present and future sense.
- ❑ Let people tell their story. Don't be satisfied with Yes or No responses.
- ❑ Let people show you how they perform their job while handling classified.
- ❑ Follow-up the check list questions with your own questions.
- ❑ Keep good notes for future reference and corrective action.

The Self-Inspection Check List

A. FACILITY CLEARANCE

1. Are the DD Forms 441 and/or 441-1 and 441s properly executed and maintained in current status? (2-111)
2. Have all changes affecting the condition of the FCL been reported to the Field Office? (1-302h)
3. Does the home office have an FCL at the same or higher level than any cleared facility within the Multiple Facility Organization? (2-108)
4. Are the senior management official, the FSO, and other Key Management Personnel cleared as required in connection with the FCL? (2-104)
5. Have the proper exclusion procedures been conducted for uncleared company officials? (2-106a-b)
6. Have the required reports been submitted to DISCO regarding employee Representatives of a Foreign Interest? (1-302d)

B. ACCESS AUTHORIZATIONS

1. Is a current record maintained of all cleared employees at each facility? (2-219)
2. Are the number of clearances held to a minimum consistent with contractual requirements? (2-200d)
3. Has a Letter of Consent (LOC) been issued for each personnel clearance (PCL)? (2-208)

4. Are all pre-employment clearance applications based on a written offer and acceptance of employment? (2-204)

5. Are all required forms and information, regarding cleared personnel, furnished to DISCO? (Chap. 2, Sec 2)

It's a good idea to retain a copy of the DISCO Form 562 used for required "Change in Cleared Employee Status Reports." This enables you to maintain a current and continuous clearance history of your cleared personnel.

6. Are employees in process for security clearances informed of their options regarding completion of the privacy portions of the DD 398, 398-2, and SF 86 application forms? (2-218)

Ensure adequate review procedures of clearance application forms to preclude error/omission and increased clearance turn-around time.

7. Does the contractor have PCLs issued to the home office facility (HOF) or has an alternative arrangement been approved by the DIS Field Office? (2-200c)

8. Does the contractor provide reports on all cleared employees to the DISCO or the DIS Field Office as required? (1-302)

C. SECURITY EDUCATION

1. Does the contractor provide all cleared employees with security training and briefings commensurate with their involvement with classified information? (1-206, 3-100 thru 3-108)

2. Are contractors who employ cleared persons at other locations ensuring the required security training? (3-104)

3. Are SF 312's properly executed by cleared employees prior to accessing classified and forwarded to DISCO for retention? (3-105)

4. Are refusals to execute the SF 312 reported to DISCO? (3-105)

5. Do initial security briefings contain the minimum required information? (3-106)

6. Does the contractor's security education program include refresher security briefings? (5-108)

Conduct personnel interviews in the work place during inspection tours of the facility and determine the effectiveness of your security education program. What do the employees remember from the last security briefing? Have them demonstrate the application of security procedures at their job function.

7. Are cleared employees debriefed at the time of a PCL's termination, suspension, revocation, or FCL termination? (3-108)

8. Has the contractor established internal procedures that ensure cleared employees' awareness of their responsibilities for reporting pertinent information to the FSO, the FBI, and other Federal authorities as required by the Manual? (1-300)

9. Does the contractor have an effective procedure for submission of required reports to the FBI, the DIS, and DISCO? (1-301, 1-302)

10. Are Government special security briefings and debriefings provided by the DIS or GCA as required? (3-103, 9-202)

11. Has the contractor established a graduated scale of administrative disciplinary action to be applied against employees who violate the Manual? (1-304)

12. Are employees aware of the Defense Hotline? (1-208)

> The Defense Hotline
> The Pentagon
> Washington, D.C. 20301-1900
>
> (800) 424-9098
> (703) 693-5080

13. Does management support the industrial security program? (1-204)

D. STANDARD PRACTICE PROCEDURES

1. Is the SPP current and does it adequately implement the requirements of the NISPOM? (1-202)

Remember that the SPP need only be prepared when the FSO or the DIS Field Office believes it necessary for the proper safeguarding of classified.

E. SUBCONTRACTING

1. Does the contractor complete all actions required in the Manual prior to release or disclosure of classified to sub-contractors? (7-101)

2. Are the clearance status and safeguarding capability of all subcontractors determined as required? (7-102)

3. Do requests for facility clearance or safeguarding include the required information? (7-101c)

4. Are all requests for facility clearance of prospective contractors based on bona fide procurement needs? (7-102d)

5. Does the contractor allow sufficient lead time between the award of a classified subcontract and the facility clearance process time for an uncleared bidder? (7-102d)

6. Does the prime contractor ensure that adequate security classification guidance is incorporated into each classified subcontract? (7-103)

7. Are contractor-prepared *Contract Security Classification Specifications* signed by a designated contractor official? (7-103)

8. Are original *Contract Security Classification Specifications* included with classified solicitations? (7-103a)

9. Are revised *Contract Security Classification Specifications* issued as necessary? (7-103b)

10. Does the prime contractor obtain approval, from the Government Contracting Agency, for subcontractor retention of classified associated with a completed contract? (7-105)

F. VISIT CONTROL

1. Can the contractor determine that all classified visits require access to or disclosure of classified information? (6-101)

2 Does notification of classified visits allow sufficient lead time for the receiver's timely approval? (6-101)

3. Do Visit Authorization Letters (VAL) include the required information, and are they updated to reflect changes in the status of that information? (6-103, 6-104)

4. Are procedures established to ensure positive identification of visitors prior to disclosure of classified? (6-105)

5. Are procedures established to ensure that visitors are only afforded access to classified information consistent with their visit (i.e., need-to-know)? (6-106)

6. Does the facility Visitor Record include the required information? (6-107)

7. Are long-term visitors governed by the security procedures of the host contractor? (6-108)

8. Has the contractor secured the approval of the relevant Government Contracting Agency prior to disclosure of classified during non-contract related visits? (6-109b)

G. CLASSIFICATION

1. Is all classification guidance adequate and is the *Contract Security Classification Specification* provided as required? (4-103)

2. Does the Government Contracting Agency issue revised *Contract Security Classification Specifications* as needed? (4-103b)

3. Does the contractor have adequate procedures for applying derivative classification to classified material being created, extracted, or summarized? (4-102)

4. Is improper or inadequate classification guidance being challenged? (4-104)

5. Upon completion of a classified contract, does the contractor properly dispose of the relevant classified information? (4-103c)

6. Is contractor-developed information appropriately classified, marked, and protected? (4-105)

7. Are downgrading and declassification actions accomplished as required, and is action taken to update records when changing the classification markings? (4-107)

H. EMPLOYEE IDENTIFICATION

1. Do personnel possess the required identification card or badge when employed as Couriers, Handcarriers or Escorts? (5-410b)

2. Do ID cards or badges, used in conjunction with Automated Access Control Systems, meet Manual standards? (5-313b)

Security procedures should maximize the use of personal recognition verification for access to classified material. Note that the NISPOM makes only passing reference to IDs and badges for use in specific instances. When such programs are employed as part of your security-in-depth procedures, the specifics should be reviewed with your DIS representative.

I. FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE

1. Is the contractor under any Foreign Ownership, Control, or Influence (FOCI) which could adversely affect performance on classified contracts? (2-301b, 2-302)

2. Has the contractor reported the presence of any/all FOCI factors to the DIS Field Office in the manner prescribed? (2-302)

3. Has the DIS Field Office been notified of negotiations for merger, acquisition, or takeover by a foreign person? (2-303b)

4. Has a FOCI Negation Plan been submitted to the DIS Field Office? (2-305)

5. Do contractor senior management officials of companies, operating under a Voting Trust, Proxy Agreement, Special Security Agreement or Security Control Agreement, meet annually with the DIS to review the effectiveness of the arrangement? (2-307)

6. Is an annual Implementation and Compliance Report submitted to the DIS Field Office? (2-307b)

7. Has a Government Security Committee been appointed from the Board of Directors under a Voting Trust, Proxy Agreement, Special Security Agreement (SSA), or Security Control Agreement (SCA)? (2-308)

8. Have companies cleared under a Special Security Agreement received the special authorization needed to access "proscribed information"? (2-309)

9. Has the contractor developed a Technology Control Plan (TCP), approved by the DIS, when cleared under a Voting Trust, Proxy Agreement, SSA, or SCA? (2-310)

J. PUBLIC RELEASE

1. Does the contractor have the approval of the Government Contracting Authority prior to public disclosure of information pertaining to a classified contract? (5-511)

2. Is a copy of each approved "request for release" retained for one inspection cycle for review by the DIS Field Office? (5-511a)

K. CLASSIFIED STORAGE

1. Has the contractor established a system of security checks at the close of each working day to ensure that classified material is secured? (5-102a)

2. Does the contractor maintain a system of perimeter controls to deter or detect unauthorized introduction or removal of classified from the facility? (5-103)

3. Are procedures developed for the safeguarding of classified material during an emergency? (5-104)

4 Is the number of persons possessing knowledge of the combinations to security containers minimized? (5-308)

5. Is a record of the names of persons having knowledge of the combinations to security containers maintained? (5-308a)

6. Are security containers, vaults, cabinets, and other authorized storage containers kept locked when not under direct supervision of an authorized person? (5-308b)

7. When combinations to classified containers are placed in written form, are they marked and stored as required? (5-308c-d)

8. Are combinations to security containers changed by authorized persons when required? (5-309)

9. Are General Services Administration-approved containers repaired as required by the Manual? (5-311)

10. Are supplanting access control systems or devices used for controlling admittance to Closed Areas during working hours? (5-312)

11. Is TOP SECRET classified stored only in approved GSA security containers, approved vaults, or Closed Areas? (5-302)

Remember, TOP SECRET classified requires supplemental protection, unless the GSA container or vault is fitted with a locking device meeting the Government FF-L-2740 standard.

12. Does the contractor provide supplemental protection for all SECRET classified not stored in GSA containers, approved vaults, or Closed Areas? (5-303)

13. Are Closed Areas constructed in accordance with the requirements of the Manual? (5-306, 5-8)

14. Has DIS approval been granted for the open storage of documents in Closed Areas? (5-306)

Intrusion Detection System Concerns

15. Do intrusion detection systems (IDS), utilized as supplemental protection, meet NISPOM requirements? (5-307, 5-900)

Remember that GSA security containers and approved vaults secured with a locking device meeting Fed. Spec. FF-L-2740 may waive the supplemental protection requirement (see 5-307c).

When guards are authorized as supplemental protection (see 5-307b), required patrol is two hours for TOP SECRET and four hours for SECRET.

16. Are Intrusion Detection Systems (IDS) approved by DIS prior to installation as supplemental protection? (5-900, 5-901)

17. Are trained alarm monitors cleared to the SECRET level and in continuous attendance when the IDS is in operation? (5-902)

18. Are alarms activated immediately at the end of business? (5-902)

19. Are alarm records maintained as required? (5-902d, e)

20. Does the Central Alarm Station report "Failure to Respond to Alarm" incidents to the DIS as required? (5-903a(3))

Commercial Central Station Alarm Company guards do not require clearance unless their duties afford them the opportunity to access classified material when responding to alarms.

21. Are all IDS at the contractor facility installed by UL-listed installers and so certified? (5-904, 5-905)

L. MARKINGS

1. Is all classified material, regardless of its physical form, marked properly? (4-200, 4-201)

2. Is all classified material marked to show the name and address of the facility responsible for its preparation and the date of preparation? (4-202)

3. Are overall markings marked conspicuously as required? (4-203)

4. Are portions of classified documents properly marked? (4-206)

5. Are all additional markings applied to classified as required? (4-202 thru 4-208)

6. Are special types of classified material marked as required? (4-210)

7. Are classification markings applied to unclassified compilations as required? (4-213)

8. Are downgrading/declassification notations properly completed? (4-216)

Holders of classified material may take automatic downgrading or declassification action as specified without further authority.

9. Does the contractor follow Manual procedure when classified material is distributed without proper classification or when it is upgraded? (4-218)

M. TRANSMISSION

1. Is classified information properly prepared for transmission outside the facility? (5-401)

2. Are receipts included when classified transmission requires? (5-401)

3. Is a suspense system established to track transmitted documents until the signed receipt is returned? (5-401)

4. Are procedures established for proper receipt and inspection of classified transmittals and are returned receipts retained for two years? (5-202, 5-204, 5-401)

5. Are authorized methods used to transmit classified outside the facility? (5-402, 5-403, 5-404)

Remember that transmission of TOP SECRET, outside the facility requires written authorization from the Government Contracting Authority.

6. Is the facility clearance and safeguarding capability of the receiving facility determined prior to transmission of classified? (2-100)

7. Are Couriers, Handcarriers, and Escorts properly briefed? (5-410)

8. Is handcarrying of classified material outside the facility properly authorized, inventoried, and safeguarded during transmission? (5-410)

9. Is handcarrying aboard commercial aircraft accomplished in accordance with required procedures? (5-411)

10. Are classified shipments made only in accordance with the Manual or instructions from the contracting authority? (5-408, 5-409)

11. Does the contractor use a qualified carrier, authorized by the Government, when shipping classified material? (5-408)

12. Are sufficient numbers of escorts assigned to classified shipments and are they briefed on their responsibilities? (5-412, 5-413)

For information concerning international transfer of classified, see International Operations (Chap. 10, Sec. 4, NISPOM).

N. CLASSIFIED MATERIAL CONTROLS

1. Do contractor employees understand their safeguarding responsibilities? (5-100)

Facility walk-throughs are a good way to determine employee knowledge of safeguarding classified when in-use. Interview and observe how classified is handled in the work place.

2. Is the contractor's information management system capable of facilitating the retrieval and disposition of classified material as required? (5-201)

Test your system for document retrieval by conducting forward and reverse checks of your classified holdings. Take a sample of classified material from your information management register and attempt to locate it within your facility. Conversely, conduct spot checks at sample locations throughout the facility where classified is stored. Identify items and determine if they are reconciled in the information management system. Remember, the inspector may no longer conduct such thorough checks, so it's up to you !

3. Are external receipt and dispatch records maintained as required? (5-202)

4. Are TOP SECRET control officials designated at facilities possessing TOP SECRET classified? (5-203)

5. Are TOP SECRET accountability records maintained as required and is an annual inventory conducted? (5-203)

6. Is all classified material received at the contractor facility and delivered directly to designated personnel? (5-204)

7. Are contractor-generated TOP SECRET documents and "working papers" entered into accountability as required? (5-205)

Remember that all classified working papers must be marked with (1) the "working paper" designation, (2) the overall classification level, and (3) the date of creation. However, accountability requirements relate only to TOP SECRET.

8. Does the contractor maintain a system of controls to deter or detect unauthorized introduction or removal of classified from the facility? (5-103)

9. Do contractor employees promptly report the loss, compromise, or suspected compromise of classified to the FSO? (1-300, 1-303)

10. Are procedures adequate to protect classified during emergencies? (5-104)

11. Are security checks conducted at the end of each working day to ensure proper storage of classified materials? (5-102)

Conduct an inspection walk-through during lunch breaks, after hours, and on late work shifts, if classified is being accessed, to determine the actual state of security at your facility.

O. CONTROLLED ACCESS AREAS

1. Do Restricted Areas have clearly defined perimeters and is all classified material properly secured when the area is unattended? (5-305)

2. Are Closed Areas approved by the DIS and properly constructed in accordance with the Manual? (5-306, 5-8)

Remember that Closed Areas require DIS, Field Office approval and an approved Intrusion Detection System (IDS) unless security guards were approved prior to this Manual. When guards are authorized as supplemental protection (see 5-307b), the required patrol is two hours for TOP SECRET and four hours for SECRET.

3. Are Closed Areas afforded adequate supplemental protection during non-working hours? (5-306, 5-307)

During non-working hours (see definition of Working Hours, Apx. C, NISPOM), Supplemental Controls are required for TOP SECRET and SECRET classified storage.

4. Do supplanting access control devices used for Closed Area access control, during working hours, meet Manual requirements and have FSO approval prior to installation? (5-312 thru 5-314)

Watch entrances to Closed Areas to determine the procedure employed when supplanting access control devices are utilized. Are authorized users allowing unauthorized persons to piggy-back into the area?

5. Are persons without the proper clearance and need-to-know escorted at all times when in a Closed Area? (5-306)

Intrusion Detection System Concerns

6. Is IDS approved by the DIS prior to installation as supplemental protection and does it meet NISPOM or UL 2050 standards as required? (Chap. 5, Sec. 9, 5-900, 5-901)

7. Are trained alarm monitors cleared to the SECRET level in continuous attendance when the IDS is in operation? (5-902)

8. Are alarms activated at the end of business? (5-902)

9. Are alarm records maintained as required? (5-902d-e)

10. Does the Central Alarm Station report failure to respond to alarm incidents to the CSA as required? (5-903a(3))

Commercial Central Station Alarm Company guards do not require a personnel clearance unless their duties afford them the opportunity to access classified material when responding to those alarms.

11. Are all IDS utilized as supplemental controls installed by UL-listed or DIS-approved installers and so certified? (5-904, 5-905)

P. DISPOSITION

1. Is a program established to review classified holdings on a recurring basis for the purpose of reduction? (5-700)

2. Is the disposition of classified material accomplished in accordance with the required schedule? (5-701)

3. Is retention authority requested as required? (5-702)

4. Is classified material destroyed as soon as possible after it has served its purpose? (5-704)

5. Does the contractor employ an effective method of destruction? (5-705)

NISPOM language does not require prior approval for any of the listed methods of destruction.

6. Is classified material destroyed by appropriately cleared contractor employees? (5-706)

The NISPOM still requires two persons for the destruction of TOP SECRET and one person for the destruction of SECRET and CONFIDENTIAL.

7. Are proper records maintained for the destruction of TOP SECRET classified and do those who sign have actual knowledge of the materials destruction? (5-707)

The NISPOM has eliminated the accountability requirement for SECRET classified material. However, keep in mind the U.S. Government reserves the right to retrieve its classified material or cause appropriate disposition. Thus, your information management system shall be capable of facilitating such retrieval and disposition in a reasonable period of time (reasonable period of time is not defined). [5-201]

8. Is classified waste properly safeguarded until its timely destruction? (5-708)

Q. REPRODUCTION

1. Does the facility's reproduction control system keep reproduction of classified material to a minimum? (5-600)

Effective access control through facility configuration, technology, and operational procedures is encouraged and should be published in the SPP.

2. Is the reproduction of classified accomplished only by properly cleared, authorized, and knowledgeable employees? (5-600)

3. Is reproduction authorization obtained as required? (5-601)

4. Are reproductions of classified material reviewed to ensure that the markings are proper and legible? (5-602)

Any review of a classified reproduction job should include concern for waste, trimmings, copy overruns, etc., and any materials used in production which may retain classified information or images requiring destruction or safeguarding.

5. Is a record of reproduction maintained for accountable material and is it retained as required? (5-603)

Remember, the NISPOM defines only TOP SECRET as accountable classified.

R. CLASSIFIED MEETINGS (sponsored by the Government)

1. Is Government sponsorship requested for classified meetings as required? (6-200, 6-201)

2. Are classified meetings held at approved locations? (6-201b)

3. Has the contractor developed adequate security procedures, for the requested meeting, and submitted them to the authorizing agency for approval? (6-201c)

4. Is attendance limited to persons cleared and having the need-to-know? (6-201c(2))

5. Is prior written authorization obtained, from the relevant Government Contracting Agency, before disclosure of classified information? (6-201c(3) and 6-202)

Remember that classified presentations shall be delivered orally and/or visually. Copies of classified presentations, slides, etc. shall not be distributed at the meeting but rather safeguarded and transmitted as required in the Manual.

6. Has a copy of the disclosure authorization been furnished to the Government agency sponsoring the meeting? (6-202b)

Authority to disclose classified information at meetings, whether by industry or government, must be granted by the Government Contracting Agency having classification jurisdiction.

7. Are contractor employees properly screened for clearance and need-to-know prior to attending a classified meeting? (6-203)

S. CONSULTANTS

For security administration purposes, the consultant shall be considered an employee of the hiring contractor or GCA. The using (hiring) contractor or GCA shall be the consumer of services offered by the consultant it sponsors for a personnel clearance.

1. Has the consultant and the using contractor or GCA jointly executed a "consultant certificate" setting forth their respective security responsibilities? (2-213)

2. Does the consultant possess classified material at his/her place of business? (2-213)

T. AUTOMATED INFORMATION SYSTEMS

1. Has the contractor obtained written accreditation from the DIS prior to processing classified on AIS? (8-102,8-200)

Protection requires a balanced approach that includes administrative, operational, physical, and personnel controls associated with the environment of the AIS. Where similar AIS are located within the same facility, a single security plan is permitted.

2. Has the contractor published and promulgated an AIS security policy that addresses the classified processing environment? (8-102b, 8-202)

3. Has an Information Systems Security Representative (ISSR) been appointed, and does that person carry out the ISSR responsibilities as defined by the Manual? (8-102)

4. Are AIS security custodians designated in facilities having multiple AIS or multiple working shifts? (8-102b(10))

5. Are security audit records maintained and reviewed at least weekly? (8-102b(9))

6. Is security awareness training provided prior to assigning an individual access to the AIS and is it part of an on-going AIS security education program? (8-202g, 8-102b(11))

Interim accreditation may be granted for a specific period of time and the contractor (ISSR) may self-approve AISs that are similar to previously accredited systems, operated in the dedicated mode, provided that the self-approval plan is included in the AISSP. For details concerning these options contact your DIS Field Office.

7. Has the ISSR determined and documented the capability of equipment not requiring AIS accreditation? (8-201)

8. Does the contractor's AIS security plan meet the standards suggested by the Manual's guidelines? (8-202)

9. Is the contractor's AIS operating in the appropriate (authorized) security mode? (8-203 thru 8-215)

AISs processing classified information must operate in one of four security modes (i.e. dedicated, system high, compartmented, or multilevel). These security modes are authorized variations in the security environment, requirements, and methods of operation.

10. Is the approved security mode for contractor AIS operation complemented by the required security features and security assurances? (8-203 thru 8-215)

11. Are appropriate physical controls being exercised over approved AIS? (8-300)

Are non-removable seals being used for protection of hardware? If so, are they occasionally checked for tampering?

12. Is software used during classified processing appropriately protected? (8-301)

13. Does the AISSP provide procedures for approval of installation of any software on the AIS? (8-301b)

14. Are AIS media containing classified handled in a manner consistent with the handling of classified documents? (8-302)

15. Are all AIS storage media, internal memory, and equipment properly sanitized and declassified prior to removal from continuous protection? (8-302)

16. Does the ISSR review, analyze, and annotate audit records associated with classified processing as specified in the AISSP? (8-302b)

17. Are audit trail records retained as required? (8-302c)

18. Are all sanitization actions verified and a record made of the date, the action taken, and the person responsible? (8-302f, 8-303a(4), 8-303c)

Authorized sanitization procedures for the most commonly used memory and storage media are defined in the Clearing and Sanitization Matrix, pg. 8-3-5 and 8-3-6, NISPOM.

19. Are instances of AIS maintenance being recorded (including addition and deletion of equipment), and are maintenance personnel appropriately cleared or escorted by knowledgeable persons? (8-303, 8-306a)

If access to classified data cannot be precluded by the escort, either the component under maintenance must be physically disconnected from the classified AIS and sanitized before and after its maintenance, or the entire AIS must be sanitized before and after maintenance.

20. Are AIS properly upgraded and downgraded where applicable? (8-304a-b)

21. Do system log-on passwords contain at least six characters and are they classified, controlled, and changed as required? (8-305b)

22. Are AISs networked at your facility? Have the additional security risks been considered? (8-403b)

23. Is an ISSR appointed for each approved network? (8-403)

24. Is the security support structure accredited for interconnected networks? (8-402)

U. COMSEC/ CRYPTO

The primary source of information for COMSEC inspections is the COMSEC Supplement to the ISM, 5220.22-S (CSISM). Paragraph reference is made to the CSISM which is now under revision, and the ISM which addresses STU-III issues. As it now stands, the NISPOM makes no reference to COMSEC.

1. Have the COMSEC custodian and one or more alternate COMSEC custodians been appointed? (Para. 12, CSISM)

2. Do the FSO, COMSEC custodian, and all alternate custodians have a final Government clearance? (Para. 8, CSISM)

3. Have the FSO, COMSEC custodian, and all alternate COMSEC custodians received a briefing within the last year by a representative of the Government? (Para. 8a, CSISM)

4. Has the GCA representative received a COMSEC briefing? (13-911, ISM)

5. Have all STU-III users been educated in its proper use and security practices? (13-911, ISM)

6. Are all installed STU-III terminals supported by a COMSEC Account? (13-902, ISM)

7. Are all STU-III terminals installed in areas which can be controlled? (13-905, ISM)

8. Are all un-keyed STU-IIIs protected as high value items? (Para. 89, CSISM)

9. Has the FSO approved the installation of all STU-IIIs for communication with other facilities? (13-905b, ISM)

10. Are FAX machines connected to STU-III terminals protected during classified processing? (13-908, ISM)

11. Are all STU-III terminals used in conjunction with classified AIS processing appropriately safeguarded and the procedures described in the AISSP? (13-910, ISM)

12. Is all Seed Key protected by the most secure manner available? (Para. 90b(4), CSISM)

13. Are all Master Crypto Ignition Keys (MCIK), if created, safeguarded in a manner commensurate with the highest classification level of the information that the master enables the STU-III to protect? (13-907b, ISM)

14. Are all Crypto Ignition Keys (CIK) stored in the same room with the STU-III safeguarded commensurate with the highest level of the information the CIK enables the STU-III to protect? (13-907c, ISM)

15. If stored in a separate room within your facility, are all CIK stored in a locked cabinet or desk as a minimum? (13-907c, ISM)

16. Is each remaining CIK, not protected in the manner above, retained in the possession of the authorized user? (13-907c, ISM)

Traditional COMSEC Accounts

1. Has a COMSEC custodian and one or more alternate custodians been appointed and briefed by a Government representative? (Para. 12a, CSISM)

2. Are the COMSEC custodian and the alternate thoroughly familiar with the duties and responsibilities outlined for them in the COMSEC SUPPLEMENT? (Para. 18a, CSISM)

3. Do the FSO, COMSEC custodian, and all alternate COMSEC custodians have a Government-granted clearance based on a background investigation conducted within the last five years? (Para 8c, CSISM)

4. Have all employees authorized access to classified COMSEC information been properly briefed? (Para. 10, CSISM)

5. Does your facility SPP contain adequate procedures for COMSEC operations at your facility? (Para. 1e, CSISM)

Are sufficient copies of the COMSEC Supplement and/or applicable equipment doctrine manuals available and adequately distributed to relevant personnel?

6. Have all COMSEC-related reports been submitted? (Sec. XVI, CSISM)

7. Has a COMSEC emergency plan been developed and approved by the CSA? (Para. 103, CSISM)

8. Have all disclosures of COMSEC information, whether to a subcontractor or other non-employees, been made only with the specific written approval of the contracting officer? (Para. 75, CSISM)

9. Is all COMSEC information in the custody of your facility properly marked and accounted for? (Para. 28, 29 and 36, CSISM)

10. Are COMSEC and keying materials marked "CRYPTO" properly stored? (Para. 90, CSISM)

11. Are COMSEC and keying materials marked "CRYPTO" properly handled in work processing areas? (Para. 88, CSISM)

12. Are access lists properly posted? (Para. 88, CSISM)

13. Is proper disposition accomplished for COMSEC and CRYPTO material? (Sec. XIV, CSISM)

14. Are COMSEC and keying materials marked "CRYPTO" properly transmitted outside the facility? (Para. 55, CSISM)

V. INTERNATIONAL OPERATIONS

Disclosure of U.S. Information to Foreign Interests

1. Does the contractor have any classified contracts with foreign interests? (If YES ... continue!)

2. Was an export license or a written letter of authorization obtained prior to disclosure of classified information? (10-200, 10-202)

Remember that an export authorization is required before the contractor makes a proposal to a foreign person that involves eventual disclosure of U.S. classified information.

3. Is proper disclosure guidance provided by the Government Contracting Authority? (10-201)

4. Are requests for export authorizations of military equipment or classified material accompanied by Department of State, Form DSP-83, Non-Transfer and Use Certificate? (10-203)

5 Has the required security clause and classification guidance been incorporated into the subcontract document for all direct commercial arrangements with foreign contractors involving classified information? (10-204)

For examples of security requirement clauses see page 10-2-4, NISPOM.

Possession of Foreign Classified Information

1. Has the DIS been notified of all contracts, awarded by foreign governments, that involve access to classified information? (10-301)

2. Is foreign government information provided protection equivalent to that required by the originator? (10-300)

Foreign government classified generally parallels our three-level system. However, occasionally you will see the marking "RESTRICTED." This material should be marked and protected as CONFIDENTIAL.

3. Are U.S. documents containing foreign government classified information marked as required by the Manual? (10-303)

4. Are contractor employees, handling foreign classified information, briefed prior to access and is it acknowledged in writing? (10-305)

5. Is foreign government material stored in a manner that prevents its mingling with other material? (10-306)

6. Is transfer of classified information outside the U.S. handled on a government-to-government basis? (10-309)

The receipt of classified material from a foreign source through non-government channels shall be promptly reported to the DIS, Field Office. (10-316)

7. Is the subcontracting of contracts involving access to foreign government information conducted in accordance with the Manual? (10-312)

International Transfers

1. Do all international transfers of classified material take place through government-to-government channels? (10-401)

2. Is an appropriate transportation plan prepared for each contract involving international transfer of classified material via freight forwarder or commercial carrier? (10-401, 10-402)

3. Does the use of freight forwarders for the transfer of classified material meet the requirements of the Manual? (10-405)

4. Is classified material handcarried outside of the U.S.? If so, is such action always approved by the DIS? (10-406)

5. Are couriers provided with a Courier Certificate and do they execute a Courier Declaration before departure? (10-406b,c)

Paragraphs (10-406a thru j) provide detailed requirements for employees acting as couriers when handcarrying classified across international boundaries.

6. Are all international transfers of classified controlled by a system of continuous receipts? (10-407)

7. Is adequate preparation and documentation provided for international transfer of classified pursuant to commercial/GCA sales or ITAR exemption? (10-408, 10-409)

International Visits and Control of Foreign Nationals

1. Has the contractor established procedures to monitor/control international visits by their employees and by foreign nationals? (10-501, 10-506, 10-507)

Visit authorizations shall not be used to employ the services of foreign nationals to access export controlled materials; an export authorization is required in such situations.

2. Are requests for visits abroad by U.S. contractors submitted on a timely basis? (10-506)

The Visit Request format is contained on pages 10-5-4 and 10-5-5.

3. Does the contractor properly control access to classified by on-site foreign nationals? (10-508, 10-509))

All violations of administrative security procedures or export control regulations by foreigners shall be reported to the CSA.

Contractor Operations Abroad

The storage, custody, and control of classified information required by U.S. contractor employees abroad is the responsibility of the U.S. Government.

1. Are employees assigned abroad properly briefed on the security requirements of their assignment? (10-604)

2. Is the CSA advised of cleared employees assigned abroad for periods exceeding 90 days? (10-605)

3. Has all transmission of classified information to cleared employees overseas been conducted through U.S. Government channels? (10-603)

Consultants shall not be assigned outside the U.S. with responsibilities that require access to classified information.

NATO Information Security Requirements

1. Are briefings/debriefings of employees accessing NATO classified conducted in accordance with the Manual, and are the appropriate certificates and records on file? (10-705)

Remember that a clearance is not required for access to NATO RESTRICTED.

2. Are all classified documents properly marked? (10-708)

3. Has the contractor received adequate classification guidance? (10-709)

4. Have the combinations to containers holding NATO classified been changed annually as a minimum? (10-711)

5. Has all NATO classified been properly received and transmitted? (10-712)

6. Are the accountability records for NATO classified maintained as required? (10-716)

7. Are visits of persons representing NATO properly handled and is the visit record maintained as required? (10-720)

W. OPSEC

1. Are OPSEC requirements implemented in accordance with contractual documentation provided by the GCA?

X. SPECIAL ACCESS PROGRAMS

1. Does the Cognizant Security Office have inspection authority for all classified programs at the facility? (see SAP Supplement)

Review of the contractor's Security Classification Guidance Specifications should identify all GCA Carve-Out programs. Remember that such programs are subject to NISPOM and Program Security Guide requirements. For more information, call your customer Program Security Office, or DIS HQ at (703) 325-6052.

Suggested Questions When Interviewing Uncleared Employees:

- ❑ What is classified information?
- ❑ Have you ever seen classified information?
- ❑ If you found classified information unprotected, what would you do?
- ❑ Have you ever heard classified information being discussed?

- ❑ Have you ever come into possession of classified materials? How?

Suggested Questions When Interviewing Cleared Employees:

- ❑ What is your job title/responsibility?
- ❑ Which contract or program requires the use of your clearance? How?
- ❑ What is the level of your security clearance?
- ❑ How long have you been cleared?
- ❑ When was your last access to classified information and at what level?
- ❑ Have you ever accessed classified information outside of this facility?
- ❑ Did anyone else from the facility accompany you on this visit?
- ❑ What procedures did you follow prior to your classified visit?
- ❑ Did you take any classified notes or classified information back to the facility?
- ❑ What procedures were followed to protect this information?
- ❑ Where is this information now?
- ❑ Have you ever provided access to classified information by visitors?
- ❑ How did you determine their need-to-know?
- ❑ Have you ever been approached by anyone requesting classified information?
- ❑ Do you ever work overtime and access classified information?
- ❑ When was the last time that you had a security briefing?
- ❑ What can you recall from this briefing?
- ❑ Can you recall any of the following being addressed in briefings?

  - Risk Management
  - Public Release
  - Adverse Information
  - Job Specific Security Brief
  - Safeguarding Responsibilities
  - Counterintelligence Awareness

- ❑ What is meant by the term adverse information and how would you report it?
- ❑ Can you recall any other reportable items?
- ❑ Have you ever been cited for a security violation?
- ❑ What would you do if you committed a security violation or discovered one?

- ❑ Do you have the combination to any storage containers, Closed Areas, etc.?
- ❑ Who other than yourself has access to these containers?
- ❑ Is a record maintained of the safe combination? If so, where?
- ❑ Do you reproduce or generate classified? If so, what controls are established?
- ❑ Where do you typically work when you generate classified information?
- ❑ What procedures do you follow to protect classified while working on it?
- ❑ Do you ever use a computer to generate classified information?
- ❑ How do you mark this information?
- ❑ Please produce the classification guidance that you used. Is it accurate?
- ❑ Are you aware of the procedures for challenging classification guidance?
- ❑ What are the security procedures for publishing classified papers, etc.?
- ❑ What procedures do you employ when handcarrying classified material?
- ❑ Have you ever reproduced classified information? Describe the procedures.
- ❑ Have you ever destroyed classified information? What procedures were used?
- ❑ Do you have any questions regarding security?

The Program Specific Self-Inspection Process

Both correspondence courses, *Essentials of Industrial Security Management* and *Protecting Secret and Confidential Documents,* identified the security concerns addressed during the self-inspections of non-possessing and possessing facilities. The scenarios described for you the self-inspection efforts of Harold Huxtable, FSO at the Electric Widget Company (EWC). Because EWC is a small facility which performs on one classified contract, any self-inspection effort would be, by default, a program specific inspection.

Are there any benefits to using the program specific approach when conducting the self-inspection of a larger facility with substantial classified involvement on a variety of programs? The program specific self-inspection can help you gain a better understanding of what your company's responsibility is for a particular classified program in addition to providing you insight as to what each person contributes to the effort. The following is provided to explain the program specific self-inspection.

Your DIS Office puts great emphasis on providing recommendations and suggestions to *improve* your security practices. But this can only be accomplished when you have a good grasp of your operations and the manner in which classified information is handled. By taking a detailed look at one or more classified programs and interviewing key individuals to determine what they do and how they handle classified information, you will be able to evaluate how well your facility's *overall* security program is functioning. Many classified programs require a variety of taskings such as manufacturing, report writing, testing, receipt, and transmission, etc. In a program specific inspection, you select one or more programs to be

closely examined. This process usually begins with the interview of the program manager (in some facilities this could even be the President) to learn what the program or contract is all about.

Start by asking for a layman's overview of the program, and question the level of classified access required, the procedures for classifying information, what, if any, problems have been experienced, and who in the facility is responsible for what on the program. This leads to interviews with other employees including technical, clerical, and secretarial personnel. During these interviews, you should explore all security requirements connected with the employee's responsibility in the program such as classified material controls, classified storage, markings, classification management, transmission, disposition, security education, and reproduction. Elements of a more administrative nature, relating to the facility's security program, such as the review of visit authorization letters and briefing statements, are ordinarily discussed separately with the FSO. *The main rule is: if the element is applicable to your facility's classified involvement, cover the element in your self-inspection and, whenever possible, consider using the program specific techniques illustrated below.*

You may find that exploring one classified program is not enough to give you a "feel" for how well your security program is functioning. One program may represent only a small part of the classified activity that takes place at your facility. If that's the case, you will want to examine several, if not all, of your classified programs in detail. It's important that you explore each inspection element thoroughly to ensure that your facility is in compliance with the NISPOM. Your underlying concern is that classified information and materials are properly protected and that your employees are knowledgeable of their security responsibilities.

A Program Specific Self-Inspection Scenario

The following scenario illustrates a self-inspection conducted on a specific program. For the purpose of this example, it is not an all-inclusive inspection.

Fenster Dinwiddie, FSO of Capabilities Limited (CL) has decided to focus his self-inspection on the SCUD Intercept Countermeasure (SIC) Project, one of three classified contracts awarded to CL. As we join Fenster, he has accomplished most of the administrative portion of the inspection. He has reviewed Letters of Consent, Briefing Statements, Personnel Security Clearance Change Notifications, etc., and has completed his inventory of all classified materials and records. He has already touched base with the President of CL to make sure there were no recent organizational changes or foreign involvement that he should report. Certain elements like Subcontracting, Consulting, COMSEC, and International Operations do not apply.

Emulating the inspection techniques formerly used by his IS Rep, Fenster has decided to go out on the floor and find out what the employees do and how knowledgeable they are about their security responsibilities. Let's listen in on some of the interviews . . .

The Program Manager Interview

Fenster recalled that his IS Rep began each inspection by interviewing the person most knowledgeable about a particular contract. In this case it means talking to Conrad Floot, the lead engineer on the SIC Project.

Fenster went upstairs to "Engineering Row" to locate Conrad. "Fenster!" cheered the engineers as he entered the department. Fenster is always tickled to receive such a salutation. He feels honored to maintain such a congenial relationship with the engineers. After all, he does represent the security department.

"Say, Conrad, can you fill me in on this SIC Project of yours? I'm doing my recurring self-inspection and decided to focus in on your program." Conrad is impressed. No one has ever expressed that much interest in his project before. And he loves to talk, especially about the SIC Project, his "baby" as he prefers to call it. "Sure, what do you need to know, Fence?"

"Well, why don't you start by giving me a program update. You know, what we're doing for the customer, what's classified about it, and things like that. But keep it simple, okay?" Conrad is thrilled. He proceeds to give Fenster a detailed overview of the program, its history, and current status. Fenster is thinking, "You know this is pretty interesting stuff. I should get out on the floor more often."

During the interview, Fenster took careful notes. He discovered that eight other engineers plus a contingent of secretarial and support personnel are working on at least some portion of the program. He decided he would interview each individual over the next couple of days. They discussed the classified design modifications which were being tested down the hall. Fenster had Conrad describe each step of the test procedure including whether aspects of the tests themselves were classified. He asked what makes the design modifications classified, how they're protected, who protects them, how and where they're tested, etc. To his relief, he found that all the procedures at least appeared to be in conformance with the NISPOM. Later, he would interview key members of the test and evaluation staff individually. He never realized there were so many security considerations!

Conrad identified his customer point-of-contact just in case Fenster or the IS Rep needed to call. They spent a lot of time on classification management. Fenster wanted to know what classification guidance had been provided by the customer and whether he felt that it was it adequate. He asked what Conrad would do if they were to experience problems in determining what should be classified. They reviewed classified marking procedures, the kind of classified information that's been received, who is allowed access, procedures for generating classified information, reproduction, disposition, transmission, public release, and access authorizations. By the time he was done, Fenster had a pretty good idea of what the SIC Project was all about and whom to talk to for more information.

In addition to addressing the program-specific security concerns, Fenster remembered to question Conrad regarding important overall security program-related issues such as security education, adverse information, and foreign travel.

Employee Interviews

Next, Fenster interviewed each of the engineers on the project. He asked many of the same questions, but this time he was more interested in learning exactly what each person's responsibilities were and how they handled classified information. He already knew a great deal about the program just by talking to Conrad. It was time to "zero in" on the nuts and bolts of the SIC Project. His first stop was at Elmo Platz's office. According to Conrad, Elmo has been involved in the program from the start and, as the assistant program head, has major responsibilities.

First, Fenster asked Elmo to explain his job and how it relates to the SIC Project. Fenster asked what level of access he needed for the job, how he obtained his classification guidance and whether there were any problems in this area that he should be aware of.

There were other questions as well, all designed to determine whether Elmo and his SIC Project staff were following the requirements of the NISPOM. Fenster asked:

- ❑ How often and under what circumstances did Elmo access classified information?
- ❑ Was he aware of his adverse information reporting responsibilities?

- ❑ Did he generate classified material in-house and, if so, on what equipment?
- ❑ How was the information protected?
- ❑ Did he have knowledge of the combination to the security container? Was the combination properly safeguarded?
- ❑ Did he attend any classified meetings at the customer's site or at CL? Did anyone else from CL attend?
- ❑ Did he reproduce classified material? On what equipment?
- ❑ Was he familiar with the rules on retention, handcarrying, "need-to-know," marking, accountability, and disposition of classified information?
- ❑ Was he aware of any unreported security violations?
- ❑ Did any of his classified work require a special briefing, e.g., NATO?
- ❑ Was there anything relating to security that he thought Fenster should know about?
- ❑ Did he have any classified information that was not logged into the facility's accountability system? Where did it come from?

You can see that Fenster was trying to cover all of the relative inspection elements listed in the self-inspection handbook during his interview. This line of questioning was continued with each of the major participants in the SIC Program, from the engineering staff to the mailroom personnel. When he was done, Fenster had covered every pertinent self-inspection element and had discovered only one or two administrative errors. His self-inspection was a success. We hope yours is, too!■

For information on the new Security Review techniques being utilized by the Defense Investigative Service ask about their Continuous Assessment, Joint Assessment, and Self-Certification security review programs.

Information Systems Security (INFOSEC) Basic 5220.22

(formerly Information Systems Security for INFOSEC Practitioners (IPC))

The course provides practice in fundamental computer security skills to support the protection of information and information systems in the Department of Defense. Given modules of instruction, practical exercises, a technical laboratory environment, and a library of reference materials, the student will be able to: Explain the threat to and vulnerabilities of information systems and employ appropriate security countermeasures to manage threat and minimize vulnerabilities; identify required physical, personnel, and procedural security procedures for information systems; and describe the elements of the information systems accreditation process. To enhance their job performance in the workplace, students will be given a "Security Information Technology User's Package" (SITUP), a collection of regulations, references, handbooks, newsletters, training aids, and agency points-of-contact.

Target audience:
Priority 1: DoD personnel assigned or projected for assignment to perform the following information systems support functions for their organization: Preventing, detecting, and eradicating viruses; auditing information systems; evaluating access controls; clearing and purging of media; and evaluating accreditation plans.

Priority 2: Employees of other Federal agencies with similar duties and responsibilities may attend the course on a space available basis.

Priority 3: Policy and oversight, inspection and/or audit, and other personnel functioning in support of Information Systems Security, on a space available basis.

Required personnel security clearance: None

Length: 5 days.

Location: DoDSI, Richmond, Virginia

Prerequisites: Students will be provided reading material before class. They will be evaluated on their comprehension of it upon entry to the course. These materials identify and define information systems technology in order to establish a common computer literacy baseline. Due to course design and time constraints, remedial training is not available.

To register: By invitation only. Nominations are validated through Information Systems Security program managers at component or agency level, identified below.

Air Force:	Call DoDSI, (804) 279-6076, DSN 695-6076.
Army:	HQDA, DISC4, (703) 696-8061, DSN 226-8061.
Navy/Marine Corps:	NISE-EAST, (803) 764-7059.
DISA:	DISA, (703) 735-8266, DSN 653-8266.

For more information on course content and attendance by other DoD agencies: Call Delmar Kerr/Christ Breissinger (804) 279-5309/3174, DSN 695-5309/3174, or Linda Braxton, Education Technician, at extension 6076. The fax extension is 6155.

SUMMARY OF NISPOM CHANGES

CHAPTER 1. GENERAL PROVISIONS AND REQUIREMENTS

1-101 Introduces the NISP and outlines principal provisions of E.O. 12829.

1-102 The Manual applies to all executive branch departments and agencies and all cleared contractors within the U.S.

1-102c Requirements of this Manual that are more costly than those previously required will be identified to the Cognizant Security Agency (CSA). The NISPOM should be implemented within six months from the date of this Manual (January 1995).

1-104 Identifies the Department of Defense, the Department of Energy, the Nuclear Regulatory Commission, and the Central Intelligence Agency as the only CSAs under the NISP.

1-105 Explains the composition of the Manual (baseline and supplement). Existing supplements to the Department of Defense Industrial Security Manual will remain in effect until revised and included in the NISPOM as annexes or until canceled.

General Requirements

1-202 Eliminates requirement to prepare Standard Practice Procedures unless required by the Facility Security Officer (FSO) or Cognizant Security Office (CSO).

1-207 Security Reviews (formerly inspections) will be conducted no more often than once every 12 months except for cause. Frequency of reviews will be based on risk management principles.

1-207a(3) Each CSA is responsible for ensuring that redundant security reviews and audit activity of its contractors are held to a minimum.

1-207b Contractor reviews (self-inspections) shall be conducted at intervals consistent with risk-management principles. No record is required.

Reporting Requirements

1-302 Reporting requirements were significantly changed to delete unnecessary reports and to consolidate similar reports.

NOTE:	For DoD contractors, reports made under 1-302 a thru g and 1-304 will be submitted to DISCO, while reports under 1-302 h thru o, and 1-303 will be submitted to the appropriate DIS Field Office.

CHAPTER 2. SECURITY CLEARANCES

Facility Clearances

2-101 A Facility Clearance (FCL) is valid on a fully reciprocal basis by all Federal departments and agencies.

2-102 Eliminates requirement to prepare a written Standard Practice Procedures as part of the FCL process.

2-104 Reduces the number of personnel clearances required in connection with the FCL.

Personnel Clearances

2-200 Within a multiple facility organization (MFO), personnel clearances will normally be issued to the home office. Cleared employee transfers within the MFO will be managed by the facility, and notification to DISCO is not required.

Eliminates redundant personnel clearance processing actions.

2-201 Instructs Federal agencies not to duplicate personnel security investigations under most circumstances.

2-203 Requires interagency reciprocity of personnel security investigations.

2-204 Permits pre-employment clearance requests up to 180 days before employment.

2-206 Eliminates the requirement to maintain a record of the evidence sighted as proof of citizenship.

2-216 Personnel clearances need no longer be summarily terminated or downgraded. Such actions shall only be taken upon termination of employment or when the need for access to classified information is reasonably foreclosed.

2-217 Concurrent clearances, reinstatement, and conversions may be accomplished using the DISCO Form 562.

Foreign Ownership, Control, or Influence (FOCI)

2-300 Major rewrite! Information includes: Foreign Mergers, Acquisitions and Takeovers, Committee on Foreign Investment In the U.S. (CFIUS), FOCI Negation Action Plans, Security Control Agreement, Technology Control Plans, and the Limited Facility Clearance.

CHAPTER 3. SECURITY TRAINING AND BRIEFING

The chapter has been reduced substantially by eliminating Defensive Security Briefing and Counterintelligence Awareness Briefing, and Extracts from Statutes and Executive Order 12356.

3-102 FSO training, if required, should be completed within one year of appointment.

3-105 Upon execution, the SF 312 (Classified Information Non-disclosure Agreement) will be forwarded to the CSA for retention.

3-106 Defensive security briefings are part of the initial and refresher briefings. They are no longer mandated prior to contact with persons from "designated countries."

3-108 Debriefing no longer requires execution of the SF 312 "Security Debriefing Acknowledgment."

CHAPTER 4. CLASSIFICATION AND MARKING

Classification

4-102 Requires that sufficient training and guidance be available to personnel authorized to perform derivative classification.

4-103b Eliminates bi-annual review and issuance of the Contract Security Classification Specification.

CHAPTER 5. SAFEGUARDING CLASSIFIED INFORMATION

Control and Accountability

5-201 Accountability for SECRET information has been eliminated. SECRET information must continue to be controlled and protected, but the record-keeping has been reduced or eliminated. Contractors have the latitude to devise a control system suitable for their unique operations.

5-205 Generated SECRET documents (working papers) no longer are accountable, but they must be marked and controlled.

Storage and Storage Equipment

5-303 Strongrooms and Class A and B vaults have been eliminated. Those in place may continue to be used.

5-306 Open shelf storage of classified documents in Closed Areas now are permitted with CSA approval and an approved Intrusion Detection System (IDS).

5-307 Approved IDS shall be used for supplemental protection for all storage containers, vaults, and Closed Areas approved for storage. Guard patrols previously approved may continue to be used.

General Services Administration (GSA) approved containers and vaults secured with a locking mechanism meeting the FF-L-2740 Federal Specification (the electronic lock) do not require supplemental protection.

5-309 Combination changes are no longer required annually or necessarily upon reassignment of an employee.

Transmission

5-401 Retention period for receipts standardized.

5-403 Uncleared commercial delivery companies may be used to transmit SECRET material with CSA approval.

5-407 Procedures for transmitting classified material within a facility are simplified.

Reproduction

5-600 Designation and posting of reproduction machines eliminated.

5-603 SECRET reproduction no longer requires record.

Retention period for TOP SECRET reproduction records reduced by one year.

Disposition and Retention

5-701 Timetable for disposing of classified material relaxed.

5-702 Classified material may be retained for two years following contract completion without written retention authorization.

When requesting retention for SECRET material, the material need only be identified by general subject matter and approximate number of documents.

5-705 Use of certain destruction equipment no longer requires CSA approval.

5-706 SECRET material may be destroyed by one person. No witness is required.

5-707 Destruction record no longer required for SECRET documents.

Construction Requirements

5-800 Closed Area and vault construction standards may conform to the NISPOM or Director Central Intelligence Directive (DCID 1/21).

Intrusion Detection Systems

5-900 Intrusion Detection Systems (IDS) shall conform to DCID 1/21 or UL 2050 standards.

5-901 IDS which do not meet these standards may remain in use until 1 January 2002.

5-902 The alarm record retention requirement has been reduced to 90 days.

5-904 IDS shall be installed by a UL-listed company or by a company approved by the CSA.

CHAPTER 6. VISITS and MEETINGS

6-103 Information required in visit authorization letter has been reduced.

6-104 Contract-related visits may be arranged for the duration of the contract.

CHAPTER 7. SUBCONTRACTING

7-102 Facility clearance verifications are valid for three years.

7-103 Eliminates bi-annual review and issuance of a Contract Security Classification Specification (DD Form 254).

7-105 Retention of classified information beyond two years after contract completion requires GCA authorization.

CHAPTER 8. AUTOMATED INFORMATION SYSTEMS (AIS)

Changes in this chapter require significant explanation. The Defense Investigative Service is preparing an Industrial Security Letter devoted to this chapter.

CHAPTER 9. SPECIAL REQUIREMENTS

When the Department of Energy (DOE) agreed to participate in the NISP, it became necessary to reconcile the differences between the way DOE and DoD handle Restricted Data (RD). Rather than increase the level of protection for all RD within DoD, it was decided to identify a category of the most sensitive RD information and provide enhanced protection to that information only. A joint DOE/DoD Nuclear Weapons Information Access Authorization Review Group was formed to identify the information to be included in this category and establish safeguards required for its protection. The Review Group was not able to complete its work prior to publication of the NISPOM and NISPOM Supplement. Therefore, Chapter 9, Section 1 in both the NISPOM and NISPOM Supplement was prepared by the DOE and reflects DOE's requirements for safeguarding RD. In addition, paragraphs 9-105b, 9-110, and 9-111 refer the reader to the NISPOM Supplement.

As the DOE requirement, if implemented within DoD, would significantly increase our security costs, DoD contractors are not to implement any changes in the way they are currently handling RD until the Review Group completes its task and new procedures are formally published for implementation.

CHAPTER 10. INTERNATIONAL SECURITY REQUIREMENTS

With the exception of the handling of Foreign Government Restricted Information, the requirements for the protection of foreign government information have not changed substantially from those in the Industrial Security Manual. However, the contents of this chapter, within the context of the remainder of the NISPOM, require considerable explanation. Therefore, the Defense Investigative Service is preparing an Industrial Security Letter devoted to international security requirements.

CHAPTER 11. MISCELLANEOUS INFORMATION

This chapter (formerly chapter 13) has been radically reduced. It retains information and requirements regarding TEMPEST, the Defense Technical Information Center (DTIC) and Independent Research and Development Efforts (IR&D).

APPENDIX C. DEFINITIONS

The following definitions have been added to or deleted from this appendix:

Added	Deleted
Affiliate	Approved Alarm System
Company	Approved Strongroom
Effectively Owned or Controlled	Candidate
Foreign Government	Complex
Government Contracting Agency	Computer Facility
Security in Depth	Computer Hardware
Transclassification	Designated Countries
U.S. Person	Executive Personnel
Voting Securities	Intending Citizen
	Limited Dissemination
	Locked Entrance
	Officers
	Personal Exchange
	Security
	Unclassified
	User Agencies

NOTE:	Most change affecting individual definitions reflects omission of examples and not a change in meaning. To be certain of any definition in the NISPOM, though, it is best to check the definition in Appendix C.

Have you heard about the

Center for Security Awareness Information?

The Department of Defense Security Institute (DoDSI) announces the 1 April 1995 inauguration of the Center for Security Awareness Information.

What exactly is this center all about?

The Center's mission is to involve the security community, both government agencies and industry, in sharing products and information to maintain and improve security awareness throughout the community. DoDSI will serve as the focal point for the center.

How do you get involved?

We ask that you submit for consideration security products or information that you or your company have developed. Our task is to make the security community aware of these products and ideas. If you know about an excellent product that you believe could or should be shared with the security community, tell us about it! We will follow-up. Through the mutual sharing of information and products, the whole security community benefits. Please get involved!

How is this going to be accomplished?

Security products referred to the DoDSI, will be reviewed and evaluated. We will then publish information about these products in the *Security Awareness Bulletin*, the *Quarterly Center for Security Awareness Information Report*, and other publications. Where appropriate, a point of contact for obtaining the product will be given. In some cases, DoDSI will provide products directly. Ultimately, we hope to provide some materials via the Internet as well as by paper copy.

What types of security products and information can you share?

We are interested in non-profit products for evaluation and broader distribution, however we will list commercial products separately in the quarterly report. Here are just a few examples of products and information you may consider submitting for review and evaluation: Videotapes, CAI/CBT software, computer games, computer graphics, computer slideshows, computer text files, films, information literature, job aids (paper products or software), manuals and handbooks, posters, print media inserts, promotional/miscellaneous items, quizzes and puzzles (paper or software), ready reference items, slide/tape sets, slides and slide sets, scripts and outlines, or services that your company is providing in the security field.

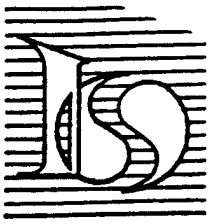
Is there a fee for submitting these products or information to the Center?

No, but we will ask each submitter, where appropriate, to sign a short release statement that gives us permission to reproduce and distribute the product.

Whom do we call to submit or discuss our security products and information?

Call Del Carrell, Manager of the Center, at (804) 279-5314 or DSN 695-5314. Or write her at:

Department of Defense Security Institute
Attn: Del Carrell
8000 Jefferson Davis Highway, Bldg. 33E
Richmond, VA 23297-5091



Interagency OPSEC Support Staff ☆ ☆ ☆ ☆ ☆

The following publications may be ordered through :

Interagency OPSEC Support Staff (IOSS)
Attn: Ms. Mary L. Hodge
6411 Ivy Lane, Suite 400
Greenbelt, MD 20770-1405
Phone: (301) 982-5411; or form may be faxed to (301) 982-2913

- ❑ National Operations Security Doctrine (NOAC Issuance)
- ❑ The National OPSEC Program
- ❑ OPSEC Program Development Procedural Guide
- ❑ OPSEC Program Evaluation
- ❑ The Great Conversation: A History of OPSEC
- ❑ Compendium of OPSEC Terms
- ❑ Operations Security Planning — A Management Tool
- ❑ Brilliant Victory — The Channel Dash of 1942
- ❑ The Operations Security Void in the Drug War (FOUO)
- ❑ Applying OPSEC to Treaty Inspections (FOUO)
- ❑ (incorporates the eight previous Treaty publications)
- ❑ Applying OPSEC to U.S. Government Contracts (New)

Please add my name to the ISSO mailing list ❑
I am currently on the IOSS mailing list ❑

Name (❑ Mr. ❑ Mrs. ❑ Ms.) (military rank): _____

Position/Title: _____

Organization: _____

Mailing address (business only): _____

_____

Phone (commercial only): ( ) _____

Contractors: Please provide the name of the Government agency sponsoring your major contract(s): _____

Computer-Based

Security Awareness Training and Education

Core security awareness briefings for industry are now available from Shadow Grafix of Lake Havasu City, Arizona

---

The following new briefing modules are currently available:

Briefing #1: *Counterintelligence Awareness Briefing* (modified version is also available for User Agencies).

Briefing #2: *Classified Information Definition and Description, Access Requirements and Need-to-know, Safeguarding, Markings, and Reproduction of Classified Material.*

Briefing #3: *Legal/Contractual Violations and Laws, Security Violations, Reporting Requirements, Travel/Seminar Advisory.*

Purchase price of $27.00 plus $1.50 for shipping and handling is the cost of software per PC installation. Site license for multiple PC installations is available. Media: 3.5" High Density Disks (1.44 MB) for IBM-compatible PCs.

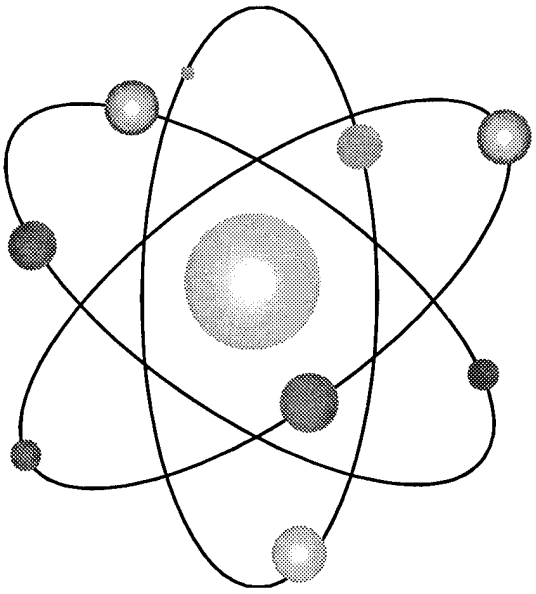
Viewers determine their own pace (approximately 15 minutes per briefing). After viewing each briefing, employees complete a Kwik Kwiz test pamphlet for the trainer to file as proof of training.

For security educators who are interested in delivering core briefings to employees by this new system:

Call or write Shadow Grafix, 1988 Thrasher Dr.,
Lake Havasu City, AZ 86404, (602)-764-3312

As always, the Center for Security Awareness Information is more than happy to announce new awareness products from commercial sources as they are made available. However, please keep in mind that this does not constitute an endorsement of the product.

Awareness Refresher Briefing



The Department of Energy, Safeguards and Security Division, has put together an Awareness Refresher Briefing, that although written for the DOE employee, is generic enough to be tailored to fit other government and industry organizations. Annual refresher briefings are not mandated by most government agencies, but they are recommended, and many security offices provide them to their employees as a good way to reinforce security awareness. The topics in this package are provided in a clear and concise outline. They include:

- Security refresher briefing introduction
- The insider threat
- The foreign intelligence threat
- Need-to-know
- Information security
- DOE policy on substance abuse or illegal drug use
- Foreign contacts
- Access authorization

- Refresher briefing guide
- Refresher briefing acknowledgment
- Briefers evaluation form

To order a copy, write to the:

U.S. Department of Energy
Personnel Security Policy Branch
Policy, Standards and Analysis Division
Office of Safeguards and Security
Germantown, Maryland 20874

Security Awareness Videos Available through The Department of Defense Security Institute

Countering Espionage Series

Three titles are available at present; others to be released in 1995-1996.
Jointly produced by DoDSI and the Intelligence Community (Project Slammer), these products are based on video-recorded interviews with espionage felons. They are aimed at empowering conscientious and loyal personnel to report or otherwise intervene in situations that might otherwise lead to the loss of classified or sensitive information or valuable assets.

#1 You Can Make a Difference emphasizes the need for co-worker intervention in the interest of fellow employees who exhibit signs of severe stress or other indicators such that their ability to safeguard critical or classified information may be in doubt.

#2 It's Not a Victimless Crime dispels the myth that espionage is some sort of white collar crime with few consequences for the offender or family members.

NEW ! ***#3 On Becoming a Spy,*** based on current research, describes how and why individuals become involved in the crime of espionage after being placed in a position of trust.

All in the Countering Espionage Series are available through FilmComm, 641 North Avenue, Glendale Heights, Illinois 60139. Phone (708) 790-3300, fax (708) 790-3325. Because the above listed products are For Official Use Only (FOUO), we ask that contractor facilities certify in their request that "This video will be used only for the training and education of employees or personnel in support of a federal government security program."

Also produced by the DoD Security Institute.....

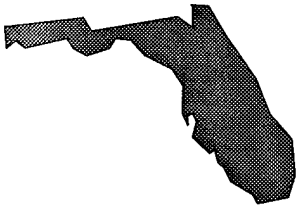
Protecting Critical Defense Information, designed for managers, executives, and senior officers who need to be reminded of their continuing security responsibilities. Narrated by Admiral William O. Studeman. (7 minutes)

This product is made available through Copymaster Video Inc., P.O. Box 684, 711 Fairfield, Villa Park, Illinois 60181. Phone (708) 279-1276. Please indicate whether payment can be made in advance by check or whether a Government Purchase Order will be used.

Other Security Awareness Videos Available from Copymaster Video.....

As Others See You, *Understanding and Reporting Foreign Intelligence Threats.* Produced by the Security Awareness and Education Subcommittee. Designed for scientific and technical employees who must protect critical technologies, and sensitive proprietary data and national security information.

Piracy in the 20th Century, *Economic & Industrial Espionage.* Produced by the Federal Bureau of Investigation, DECA Program, especially for the defense contractor community, this video examines the threat by so-called friendly foreign interests to critical U.S. technology.



INDUSTRIAL SECURITY AWARENESS COUNCIL

AWARENESS EDUCATION COMMUNICATION COOPERATION

Florida Space Coast Chapter

SECURITY BULLETIN **MARCH 1995, NO. 016**

A BRIEF ON BRIEFINGS

Briefly, there are three different types of briefings required by the NISPOM for cleared employees. *Initial* Security Briefing must be given prior to employees being granted access to classified information. This briefing must include:

- A Threat Awareness Briefing
- A Defensive Security Briefing
- An overview of the Security Classification System
- Employee reporting obligations and requirements
- Security procedures and duties applicable to the employee's job

Refresher briefings, the second type, must be conducted periodically. As a minimum, this briefing will reinforce the information provided during the initial briefing and inform employees of appropriate changes in security regulations. Contractors must satisfy the requirement by use of audio/visual materials and by issuing written materials on a regular basis, such as these bulletins.

The third briefing, *debriefing*, is required at the time of termination of employment, such as, discharge, resignation, retirement, or when an employee's personal clearance is terminated, suspended, administratively terminated or revoked and upon termination of the facility clearance.

Initial, refresher and debriefings must also be provided by temporary help suppliers - specifically, a temporary help supplier, or other contractor who employs cleared individuals solely for dispatch elsewhere. The temporary help supplier or the using contractor may conduct these briefings.

The **NISPOM** requires you to brief cleared personnel. The purpose of the three briefings is to ensure employees thoroughly understand their responsibilities for the protection of classified information and the possible consequences to our nation for failure to satisfy these objectives.

It's time to start planning! — November 30th will be the eighth annual observance of

Computer Security Day

An opportunity to focus attention on the critical area of computer security

Computer Security Day is the final workday in November, although official observances vary to avoid conflicts in some countries or in some organizations. As the holiday season approaches and security might otherwise become lax, Computer Security Day reminds everyone to follow proper computer security procedures. It's the perfect opportunity to announce new aspects of your organization's computer security program.

This year, more than 1000 organizations from around the world will officially participate. To make your organization an official participant this year, simply send a note on your company's stationery to:

Association for Computing Machinery
Special Interest Group on Security Audit and Control
Computer Security Day Committee
Post Office Box 39110
Washington, DC 20016 USA

You will receive, at no cost, a list of suggested activities and a new computer security poster you can use to help draw attention to this vital concern.

You Can Host These Courses On-site at Your Facility (Industry or Government)

Train-the-Trainer Course (TTT) 5220.13A, 4.5 days

Purpose: To train you to *teach* the SBC. This workshop, conducted on the 2 days before a scheduled SBC, prepares you to be an instructor for the SBC. You will receive instruction by DoDSI staff on how to:

- use the SBC materials;
- present selected lessons in the SBC;
- facilitate the preparation of briefings;
- conduct practice briefing sessions; and
- evaluate live briefings.

Under DoDSI supervision, you will then spend the next 2.5 days teaching your first SBC.

Security Briefers Course (SBC) 5220.13, 2.5 days

Purpose: To improve your effectiveness as a security education briefer. You will receive instruction on how to:

- prepare a briefing plan;
- design and use briefing aids;
- present your briefings in a clear and interesting manner; and
- evaluate live briefings.

As the "Security" in the course title suggests, the briefings presented by you in class must address security requirements, but the real emphasis of the course is on accomplishing the above objectives so that you become more skilled and more comfortable at speaking in front of others.

If you are considering participating in the TTT, it is suggested that you: Be responsible for your organization's security briefing program; be an experienced security briefer or a graduate of the SBC; have a need to train others to prepare and present security briefings; and have a working knowledge of security requirements. If you want to learn *how* to brief—choose the SBC.

To host the courses described above, please call Linda Braxton or Gussie Scardina, DoDSI, at (804) 279-6076/5308 or DSN 695-6076/5308.

These courses are held in succession. The TTT precedes the SBC.

To host the SBC, you must be able to provide:

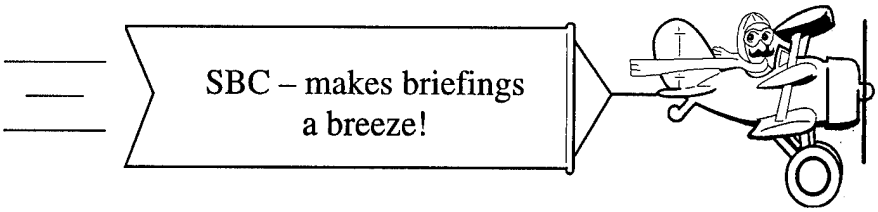
- ☐ one main classroom for 24 students
- ☐ 3 breakout rooms for 6 students each
- ☐ A-V equipment for all 4 rooms
  (Overhead projectors, screens, and writing surfaces for each room)
- ☐ At least two of the instructors and preferably more for the TTT.
- ☐ An on-site coordinator
- ☐ Invitations to other security organizations in your area in order to fill a class of 24.

The Department of Defense Security Institute (DoDSI) will:

- ✔ Provide the lead instructor and assume responsibility for the teaching success of the course.
- ✔ If necessary, provide security personnel from other organizations to help teach the course.
- ✔ Provide two full days of training for the instructors prior to starting the course.
- ✔ Provide the instructional materials in sufficient quantities for 24 students.
- ✔ Help the trainers teach the Security Briefers Course.

Here's your chance to sign up for the

Train-the-Trainer/Security Briefers Course!



August 21-25, 1995
Air Reserve Base, Indiana
POC: Mr. Kirk Bireley
101 Lighting Grissem
Air Reserve Base, IN 46971-5000
(317) 688-8589
DSN 928-8589

September 11-15, 1995
Colorado Springs, Colorado
POC: Angelique Phillips
Defense Investigative Service
(719) 260-1655

We also have one course that will be taught at the DoD Security Institute

Train-the-Trainer	**Security Briefers Course**
September 25-29, 1995	September 27-29, 1995

The dates below are open and available to anyone wanting to host the Train-the-Trainer/Security Briefers Course. If interested, Linda Braxton will give you the full details to help you put a class together. Give her a call on (804) 279-6076, DSN 695-6076.

July 31-August 4, 1995

August 28-September 1, 1995

Security Awareness Publications Available from the Institute

Publications are free. Just check the titles you want and send this form to us with your address label

Our address is:

DoD Security Institute
Attn: SEAT
8000 Jefferson Davis Hwy, Bldg 33E
Richmond, VA 23297-5091
(804) 279-5314 or DSN 695-5314

- ❑ **Recent Espionage Cases: Summaries and Sources**. July 1994. Eighty-five cases, 1975 through 1994. "Thumb-nail" summaries and open-source citations.
- ❑ **DELIVER!** Easy-to-follow pamphlet on how to transmit and transport your classified materials. Written specifically for the Department of Defense employee.
- ❑ **Terminator VIII**. Requirements for destruction of classified materials. Contains questions and answer for some common problems and also detailed information on various destruction methods. Written specifically for the Department of Defense employee.
- ❑ **STU-III Handbook for Industry**. To assist FSOs of cleared defense contractors who require the STU-III, Type 1 unit. Covers step-by-step what you need to know and do to make the STU-III a valuable addition to your facility's operations.
- ❑ **Survival Handbook**. The basic security procedures necessary for keeping you out of trouble. Written specifically for the Department of Defense employee.
- ❑ **Layman's Guide to Security**. The basic security procedures that you should be aware of when handling classified materials in your work environment.
- ❑ **Acronyms and Abbreviations**. Twelve pages of security-related acronyms and abbreviations and basic security forms.

Security Awareness Bulletin. A quarterly publication of current security countermeasures and counterintelligence developments, training aids, and education articles. Back issues available from the Institute:

- ❑ The Case of Randy Miles Jeffries **(2-90)** Jan 90
- ❑ Beyond Compliance - Achieving Excellence in Industrial Security **(3-90)** Apr 90
- ❑ Foreign Intelligence Threat for the 1990s **(4-90)** Aug 90
- ❑ Regional Cooperation for Security Education **(1-91)** Jan 91
- ❑ AIS Security **(2-91)** Sep 91
- ❑ Economic Espionage **(1-92)** Oct 91
- ❑ OPSEC **(3-92)** Mar 92
- ❑ What is the Threat and the New Strategy? **(4-92)** Sep 92
- ❑ Acquisition Systems Protection **(1-93)** Apr 93
- ❑ Treaty Inspections and Security **(2-93)** Jul 93
- ❑ Research on Espionage **(1-94)** Mar 94
- ❑ Information Systems Security **(2-94)** Aug 94
- ❑ Acquisition Systems Protection Program **(3-94)** Oct 94
- ❑ Aldrich H. Ames Espionage Case **(4-94)** Dec 94
- ❑ Revised Self-Inspection Handbook/Summary of NISPOM Changes **(1-95)** Jul 95

*U.S. Government Printing Office: 1995 — 628-109/40001

Department of Defense Security Institute
8000 Jefferson Davis Highway, Building 33E
Richmond, Virginia 23297-5091

Official Business
Penalty for Private Use $300

THIRD CLASS
POSTAGE & FEES PAID
DEFENSE INVESTIGATIVE SERVICE
PERMIT NO. G-131